

LFC Requester:	Theresa Rogers
-----------------------	-----------------------

**AGENCY BILL ANALYSIS
2016 REGULAR SESSION**

WITHIN 24 HOURS OF BILL POSTING, EMAIL ANALYSIS TO:

LFC@NMLEGIS.GOV

and

DFA@STATE.NM.US

{Include the bill no. in the email subject line, e.g., HB2, and only attach one bill analysis and related documentation per email message}

SECTION I: GENERAL INFORMATION

{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Check all that apply:

Original X **Amendment**
Correction **Substitute**

Date 22 January 2016

Bill No: SB 154

Sponsor: Peter Wirth and Jim Dines

Agency Code: 305

Short Electronic Communications

Person Writing Kenneth H. Stalter

Title: Policy Act

Phone: 505 222 9056 **Email** kstalter@nmag.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY16	FY17		

(Parenthesis () Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY16	FY17	FY18		

(Parenthesis () Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY16	FY17	FY18	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total						

(Parenthesis () Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to: May conflict w/ a variety of laws. See below.

Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

This analysis is neither a formal Attorney General's Opinion nor an Attorney General's Advisory Letter. This is a staff analysis in response to an agency's, committee's, or legislator's request.

Synopsis:

This bill creates the state Electronic Communications Privacy Act. The Act generally prohibits a government entity from gaining access to or compelling production of electronic data held in electronic communications devices or by service providers. These terms are defined broadly, such that the bill appears to apply generally to all data held in electronic form, whether by an end-user or by a third party.

Under the terms of the Act, a government entity may access information held by a third party only with a warrant or with a wiretap order. A government entity may access information on a device only with a warrant, with a wiretap order, with consent of the device's "authorized possessor," if the device is lost or abandoned, or in case of an emergency.

Any warrants issued for electronic data under this Act must require that any information obtained is "destroyed within thirty days" unless the information is "exculpatory" or related to the "the objective of the warrant." Courts are authorized to appoint special masters to facilitate this requirement.

A service provider may voluntarily disclose data if allowed by law. The government entity receiving this information, however, must destroy it within ninety days unless it obtains consent of the sender or recipient or a court order.

In the event that a government entity obtains electronic information due to an emergency, the government must, within three days, apply for a warrant or order from the court authorizing the production of the information.

The Act states that it does not limit the authority of a government entity to "use an administrative, grand jury, trial or civil discovery subpoena" to obtain (1) information about a communication from the sender or recipient of that communication; (2) information about a communication made by an officer, director, employee, or agent of an entity that provides communication services to its officers, directors, employees, and agents; or (3) subscriber information from a service provider. "Subscriber information" is defined as contact information of the subscriber, account numbers, and the length and type of service.

Recipients of electronic communications are allowed to voluntarily disclose information about the communications to the government.

The Act requires that when a government entity obtains information under a warrant or due to an emergency, the government entity must provide notice to the identified target. If there is no identified target, the government entity must provide the required information to the Office of the Attorney General, which must post the information (with identifying details redacted) on a

website. A court may authorize delayed notification if notice could result in “adverse results” including tampering with evidence, flight from a jurisdiction, jeopardy to an investigation, danger to a person, or intimidation of a witness.

The Act provides that if it is violated, any evidence may be suppressed at trial. Recipients of warrants, orders, or other legal process that violate the bill may move for destruction of the evidence. The Act also authorizes the Attorney General to enforce the Act through civil proceedings.

Finally, the Act requires any government entity that obtains electronic communication information to submit annual reports to the Office of the Attorney General. The reports must include the number of times information was sought, the number of different types of information sought, the number of persons whose information was sought and other details. The Act requires the Office of the Attorney General to public these reports on its website, along with a summary compilation of all reports received.

FISCAL IMPLICATIONS

SIGNIFICANT ISSUES

The Act requires law enforcement agencies to destroy evidence obtained in criminal investigations. This could result in violation of a criminal defendant’s due process rights. Generally, “the State has a duty to preserve evidence obtained during the investigation of a crime.” *State v. Pacheco*, 2008–NMCA–131, ¶ 28, 145 N.M. 40. The Act attempts to reconcile this by requiring the government entity to preserve “exculpatory information.” It is unlikely, however, that law enforcement agencies will be able to determine what evidence may later turn out to be exculpatory. This is for several reasons. During a long-term investigation, evidence often only takes on significance in light of other evidence obtained at a later date. Law enforcement agencies cannot anticipate what a defendant’s theory of the defense may be. In a complex case with multiple suspects, evidence that is irrelevant as to one suspect may later be claimed to be “exculpatory” as to another. Finally, once evidence has been destroyed, it becomes very difficult to evaluate claims that it was actually exculpatory and should have been preserved. Overall, this puts law enforcement in a difficult position. Agencies will have to labor under dual duties to both preserve and destroy evidence without knowing where the lines may later be drawn.

The Act may conflict with or be pre-empted by the federal Electronic Communications Privacy Act. 18 U.S.C. 2703. The federal Act generally establishes a framework for governmental entities, including State entities, to obtain data held by third-party providers. Depending on the information sought, the federal Act allows it to be obtained through warrant, court order, or subpoena. This bill would create a situation where disclosure was authorized under the federal Act but prohibited under the state Act. This potential conflict is compounded by the fact that the state Act makes no provision for extraterritorial application. Given that many service providers are located out of state, this creates a serious question as to whether warrants or orders directed at those providers are governed by the state Act or the federal Act.

The state Act may also conflict with the grand jury statutes, which generally afford the grand jury broad powers to subpoena “all public and private records or other evidence relevant to its inquiry.” NMSA 1978, § 31-6-12 (1979). Under the Act, a grand jury would be limited to seeking information from the recipient of a message, information from an entity about its employees, or solely subscriber information. This could hamper the traditional investigative role of the grand jury.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

The Act could impose administrative burdens on law enforcement agencies as they will be required to revamp their procedures relating to digital evidence. Given the potentially expansive application of the Act, this could impact the prosecution of any case involving digital evidence. The number of cases involving digital evidence is likely to grow in the future. For example, even a routine shoplifting case may involve digital video from the store, which could fall under the ambit of this Act's broad definitions.

The Act could also impose administrative burdens on the Office of the Attorney General, which is tasked with collecting, compiling, and publishing statistics from all agencies in the state that obtain any evidence covered by the Act.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

May Conflict with the federal Electronic Communications Privacy Act. 18 U.S.C. 2703; rules for grand jury investigations and other laws such as the child solicitation by electronic communication device statute, NMSA 1978, § 30-37-3.2. [See discussion above.]

TECHNICAL ISSUES

The Act may also be construed more broadly than intended. A number of technical terms are defined and the relations between them are not always clear. The end result could be an expansive application of the law.

Under the current definitions, a service provider appears to mean any entity offering the opportunity for users to transfer data, images, sounds, or other signals in an electronic form. The definition of electronic information includes the contents of electronic communications, which in turn includes "a sign, a signal, a writing, an image, a sound, a datum or intelligence of any nature."

Together, these definitions suggest that the Act applies to essentially any data stored or communicated in electronic form. That would include everything from internet service providers to coffee-shops offering wi-fi to electronically stored healthcare records to 911 calls to bank records to digital surveillance video at big box stores.

OTHER SUBSTANTIVE ISSUES

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

If this bill is not enacted, requests for electronic information will continue to be governed by a wide variety of constitutional and statutory limits, including both federal and state constitutions, the federal Electronic Communications Privacy Act, the federal Stored Communications Act, the recently enacted federal Cybersecurity Information Sharing Act, the state and federal wiretap statutes, and the rules of criminal procedure.

AMENDMENTS